УДК 004.056
DOI https://doi.org/10.32689/maup.it.2024.1.5

Андрій ГЛАЗУНОВ
аспірант спеціальності 122 «Комп'ютерні науки»,
Національний університет біоресурсів і природокористування України,
glasgarick2013@gmail.com
***ORCID:** 0009-0003-8631-8430*

ОГЛЯД ТА АНАЛІЗ ДОСЛІДЖЕНЬ З ПРОБЛЕМАТИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ХМАРНИХ ІНФРАСТРУКТУР

Анотація. *Хмарні обчислення є моделлю забезпечення доступу до мережевих ресурсів, таким як сховища даних і обчислювальні потужності на вимогу, без прямого управління з боку користувачів. В даний час хмарні обчислення включають як публічні, так і приватні центри обробки даних, що надають клієнтам єдину платформу через інтернет. Периферійні обчислення (edge computing) – це стратегія, спрямована на наближення виконання обчислень та збереження інформації до кінцевих користувачів, скорочення часу відгуку та оптимізації пропускної спроможності хмарних сервісів. Мобільні хмарні обчислення використовують розподілені обчислення для передачі програм на мобільні пристрої, такі як телефони та планшети. Численні дослідження показують, що хмарні обчислення і мобільні хмарні обчислення стикаються з проблемами інформаційної безпеки (ІБ), загрозами та вразливістю для клієнтів, і одним із перспективних методів боротьби з цими загрозами є використання методів машинного навчання (МН). У цій статті проведено аналіз загроз та проблем з ІБ, а також виконано огляд, запропонованих різними авторами рішень, щодо забезпечення ІБ хмарних обчислень та хмарних сервісів. Насамперед, розглянуто дослідження, що ґрунтуються на застосуванні алгоритмів МН для забезпечення безпеки хмарних обчислень та хмарних сервісів.*

Ключові слова: *хмарні обчислення; інформаційна безпека; машинне навчання; кібератаки, аномалії.*

Andrii HLAZUNOV. REVIEW AND ANALYSIS OF RESEARCH ON THE ISSUES OF INFORMATION SECURITY OF CLOUD INFRASTRUCTURES

Abstract. *Cloud computing is an access to network resources, such as data storage and computing power, on demand, without direct control by users. Currently, cloud computing includes both public and private data centers that provide customers with a single platform over the Internet. Peripheral computing (edge computing) is a strategy aimed at bringing computing and information storage closer to end users, reducing response time and optimizing the bandwidth of cloud services. Mobile cloud computing uses distributed computing to deliver applications to mobile devices such as phones and tablets. Numerous studies show that cloud computing and mobile cloud computing face information security (IS) challenges, threats, and vulnerabilities for customers, and one of the promising methods to combat these threats is the use of machine learning (ML) techniques. In this article, an analysis of IS threats and problems is carried out, as well as a review of the solutions proposed by various authors for the IS provision of cloud computing and cloud services. First of all, research based on the application of MN algorithms to ensure the security of cloud computing and cloud services is considered.*

Key words: *cloud computing; informational security; machine learning; cyber attacks, anomalies.*

Вступ. Хмарні обчислення з'явилися відносно нещодавно, як нова структура для спрощення та надання послуг через Інтернет [22]. Організація хмарних обчислень включає розміщення одного або декількох центрів обробки даних (ЦОД), які взаємопов'язані між собою. Ця система спроектована таким чином, що для користувача немає різниці між фізичними компонентами системи та їх віртуальними уявленнями. Завдяки цьому користувач хмарних обчислень може взаємодіяти з обчислювальними ресурсами, не турбуючись про технічні деталі та організацію процесу, оскільки ці завдання повністю покладаються на оператора хмарного сервісу. Фінансові обмеження, пов'язані з оптимізацією витрат приватних та державних структур (у загальному випадку об'єктів інформаційної діяльності – ОІД), а також зростаючі потреби в обчислювальних ресурсах, вимагають зростання обсягів сховищ даних із паралельним збільшенням потреб в аналізі. Ці та інші чинники сприяли розширенню попиту на різні хмарні моделі [10, 13]. Однак, як було показано в роботах [24, 30] хмарні обчислення та хмарні сервіси, мають низку проблем із забезпеченням інформаційної безпеки (ІБ). Зауважимо, що з точки зору ІБ є певна різниця між забезпеченням ІБ хмарних обчислень і хмарних сервісів. Ці відмінності можна звести до таких категорій:

1. Рівень контролю ІБ для хмарних обчислень та хмарних сервісів. У хмарних обчислень клієнти мають великий контроль за безпекою своїх даних і додатків, тоді як у хмарних сервісів більше контролю за безпекою, має провайдер. У хмарних сервісів, клієнт може мати досить обмежені можливості для налаштування та управління політиками безпеки.

2. Поверхня атаки для хмарних обчислень та хмарних сервісів. У хмарних обчислень клієнтська інфраструктура та програми можуть бути вразливими перед атаками, зокрема мережевими. У той же час

для хмарних сервісів поверхня атаки, як правило, набагато менша, оскільки провайдер відповідає за ІБ своєї інфраструктури.

3. Відповідність хмарних обчислень та хмарних сервісів. У хмарних обчисленнях клієнти безпосередньо повинні відповідати вимогам безпеки. У хмарних сервісів тільки провайдер несе відповідальність за дотримання вимог ІБ.

Таким чином, хмарні обчислення та хмарні сервіси мають дещо відмінні моделі безпеки. Вибір конкретної моделі залежатиме від потреб клієнта, його технічної експертизи та вимог до безпеки. Все сказане вище і мотивувало виконати аналіз наукових публікацій, присвячених виключно проблематиці забезпечення ІБ хмарних обчислень і хмарних сервісів.

2. Огляд попередніх досліджень.

У [17] автори розглядають загальний алгоритм вирішення проблем безпеки підвищення продуктивності хмарної системи. Автори використовували штучні нейронні мережі (ШНМ) для аналізу захищеності хмарного середовища.

У [19] розглядається організація системи безпеки хмарних обчислень, заснована на довірі, у хмарних моделях. Тобто провайдер забезпечує надійність, безпеку та конфіденційність даних у хмарній системі. Авторами запропоновано модель управління доступом на основі довіри як ефективний метод забезпечення ІБ у розподілених обчислювальних інфраструктурах. Як клієнтські, так і хмарні активи клієнтів у хмарної системі, у цьому дослідженні оцінюються з урахуванням аналізу їх довіри.

У [31] аналізуються моделі забезпечення ІБ хмарної інфраструктури. Автори розглянули у своїй роботі відмінні проблеми ІБ розподілених обчислень, що виникають у результаті використання об'єктами інформаційної діяльності різних моделей хмарних обчислень. Як показано авторами, приватні хмари зазвичай використовуються організаціями для своїх внутрішніх потреб. Вони вимагають суворого контролю доступу та управління. Громадські хмари надаються сторонніми провайдерами і можуть бути менш прозорими щодо безпеки. У громадських хмарах ресурси можуть розподілятися між різними клієнтами. Це потребує додаткових заходів безпеки.

У [9] автори розглядають моделі машинного навчання (далі МН) підвищення безпеки даних у хмарних системах. Концепція забезпечення ІБ розподілених обчислень обговорюється авторами в контексті віртуалізації серверних ферм як практичного середовища розгортання бізнес-додатків. На думку авторів, віртуалізація серверних ферм допомагає забезпечити безпеку хмарних обчислень шляхом ізоляції, оскільки віртуальні сервери у фермі можуть бути ізольовані один від одного, запобігаючи несанкціонованому доступу (НСД). Крім того, ферма може динамічно масштабуватись в залежності від навантаження, забезпечуючи гнучкість та ефективність. Віртуальні сервери можуть мати різні рівні доступу, що сприяє безпеці.

У [37] автори наводять модель класифікації загроз для хмарних обчислень. Особливість класифікації полягає в тому, що вона заснована на можливості алгоритмів МН для виявлення та вирішення проблем безпеки. Крім того, авторами пропонується модель угруповання ризиків для хмарних обчислень. Модель ґрунтується на алгоритмах МН.

Аналогічні дослідження були проведені в роботі [13]. Дослідження присвячене аналізу сучасних підходів, вкладених у забезпечення ІБ хмарних сервісів. З огляду на те, що хмарні обчислення є однією з найбільш зростаючих областей у сфері інформаційних технологій, забезпечення безпеки та надійності процесів, що відбуваються у хмарах, а також захист механізмів взаємодії між клієнтами та постачальниками хмарних сервісів, становлять вкрай важливе наукове та прикладне завдання. Побоювання щодо втрати даних та їх компрометації стоять біля витоків небажання деяких компаній переміщати свої обчислення до хмар. Автор аналізує різноманітність хмарних сервісів, що надаються різними провайдерами, та порівнює існуючі підходи до забезпечення ІБ у цій сфері. Крім того, пропонується новий підхід, що базується на принципі диверсифікації. На думку автора, застосування диверсифікації необхідне забезпечення надійності та безпеки критичних компонентів хмарних систем. Цей принцип полягає у використанні унікальної версії кожного ресурсу завдяки особливій комбінації провайдерів хмарних обчислень, географічного розміщення центрів обробки даних, моделей надання хмарних сервісів та моделей розгортання хмарної інфраструктури.

У [29] автори досліджують алгоритми МН, які можуть бути використані для усунення загроз ІБ, пов'язаних із поширенням шкідливого програмного забезпечення (ПЗ) у хмарних системах. Авторами запропоновано бар'єрну структуру, яка використовує три алгоритми МН та призначена для виявлення шкідливого ПЗ.

Як було показано в [19, 35] хмарні обчислення мають значний потенціал для зростання і стає все більш популярними. Однак, незважаючи на свої унікальні характеристики, хмарні обчислення пов'язані з різними загрозами безпеці. Категоризація загроз була виконана багатьма авторами, зокрема у роботах [13, 19, 35].

Загрози конфіденційності включають інсайдерські загрози для клієнтської інформації, а також ризики зовнішніх атак [14]. [14] показано, що, по-перше, інсайдерський ризик для клієнтської інформації, пов'язаний з несанкціонованим або незаконним доступом до інформації про клієнта з боку інсайдера постачальника хмарних послуг. Це серйозна проблема безпеки [19]. По-друге, ризик зовнішніх атак стає дедалі актуальнішим для хмарних обчислень. Цей ризик включає віддалені програмні або апаратні атаки, спрямовані на клієнтів та хмарні програми [14]. По-третє, витік інформації є необмеженим ризиком для хмарних даних через навмисні та/або ненавмисні людські помилки.

Загрози цілісності інформації з організацією хмарних обчислень розглянуті у роботах [16, 31]. По-перше, це ризик ізоляції інформації, яка неточно поєднує значення параметрів безпеки, необачне проектування віртуальних машин (ВМ) та зовнішні клієнтські гіпервізори. По-друге, це погане управління доступом клієнтів, яке через неефективний контроль доступу може зіткнутися з різними проблемами та загрозами ІБ. Що дозволить потенційним зловмисникам завдати шкоди інформаційним активам, розміщеним у хмарі [5, 20].

Як показано в [12, 20] загрози доступності включають, наприклад, фізичне переривання роботи хмарних обчислень та/або хмарних сервісів, а також пов'язані з неефективними стратегіями відновлення після атак на хмарні системи.

У роботах [1, 2, 4, 18, 23, 34] аналізуються різні види атак на хмарні системи. У [18] обговорюються сценарії мережевих атак. Зокрема, як зазначають автори, сканування портів становить для хакерів значний інтерес, оскільки дає інформацію про запуск успішної атаки. У [34] розглядаються спуфінг-атаки при яких хакер чи шкідливе ПЗ діють від імені іншого користувача (або системи), видаючи себе за дані.

У [18] також розглянуті особливості організації атак на основі ВМ. У роботі показано, що різні ВМ, що використовуються у хмарних платформах, можуть викликати різні проблеми з ІБ. Наприклад, у разі, коли шкідливий код, розміщений в середині образу ВМ, буде реплікований під час створення ВМ. Також автори аналізують атаки з урахуванням додатків, які у хмарі. Такі атаки можуть вплинути на його продуктивність хмарних додатків і спричинити витік інформації в зловмисних цілях.

Як самостійний напрямок досліджень із проблематики ІБ хмарних інфраструктур можна вважати роботи, пов'язані із застосуванням методів МН для забезпечення ІБ хмарних обчислень.

Згідно [11] машинне навчання – це логічна перевірка розрахунків та вимірних моделей, які комп'ютерні системи використовують для реалізації конкретного завдання.

З погляду ІБ методи МН [27] настільки значущі у хмарі, що у найближчому майбутньому кожна хмарна система використовуватиме методи МН. Зі збільшенням затребуваності хмарних обчислень та зростанням навантаження на систему, а також обсягу трафіку стає необхідним активне моніторингове втручання в роботу ЦОД. Це дозволяє забезпечити безперебійну роботу інфраструктури, оскільки оперативне реагування на загрози ІБ та несправності сприяє стабільності та безпеці системи. Моніторинг, включаючи відстеження стану компонентів та управління хмарною інфраструктурою, відіграє ключову роль у забезпеченні високого рівня послуг, оптимізації розподілу ресурсів та забезпеченні надійності та ІБ. Це однаково важливо як для клієнтів, так і для провайдерів хмарних послуг. Моніторинг хмарного середовища включає кілька підтипів, кожен з яких виконує свої функції [18]. Зокрема, моніторинг ІБ – виявлення потенційно небезпечних алгоритмів та запобігання порушенням безпеки хмарних систем.

Для ефективної побудови системи моніторингу необхідно розробити математичну модель, що ґрунтується на оцінці параметрів системи в різних станах та часі, а також на основі застосування методів МН. Такий підхід дозволить створити формальний апарат із вхідними, проміжними та вихідними станами, що сприятиме забезпеченню ІБ як хмарних обчислень загалом, так і хмарних сервісів, зокрема.

У роботах [26, 32, 36] розглядаються інстанси хмарної інфраструктури у контексті забезпечення ІБ хмарних обчислень. Інстанси є віртуальними або фізичними обчислювальними ресурсами, що надаються хмарним провайдером для виконання різних завдань і додатків. Ці ресурси можуть включати ВМ, контейнери, сервери, бази даних (БД) та інші обчислювальні ресурси, які можуть бути масштабовані та налаштовані відповідно до потреб клієнта. На думку авторів [26], інстанси (ВМ або контейнер) хмарної інфраструктури відіграють важливу роль у забезпеченні ІБ хмарних сервісів, див. рис. 1.

По-перше, провайдери часто використовують віртуалізацію для створення та управління інстансами хмарної інфраструктури. Це дозволяє забезпечити ізоляцію та сегментацію ресурсів між різними клієнтами, що допомагає запобігти НСД до даних та додатків. По-друге, інстанси хмарної інфраструктури можуть використовуватися для виявлення аномалій, потенційних загроз та несанкціонованих дій. Це дозволяє операторам хмарних сервісів оперативно реагувати на можливі інциденти безпеки та запобігати їм. По-третє, використання інстансів також дозволяє налаштовувати права доступу та політики ІБ для різних користувачів та програм. Це забезпечує контроль над доступом до даних та ресурсів та допомагає запобігти НСД. По-четверте, інстанси можуть бути налаштовані за допомогою

спеціалізованих засобів захисту від DDoS-атак, що допомагає забезпечити безперервність роботи сервісів навіть при масованих мережевих атаках.

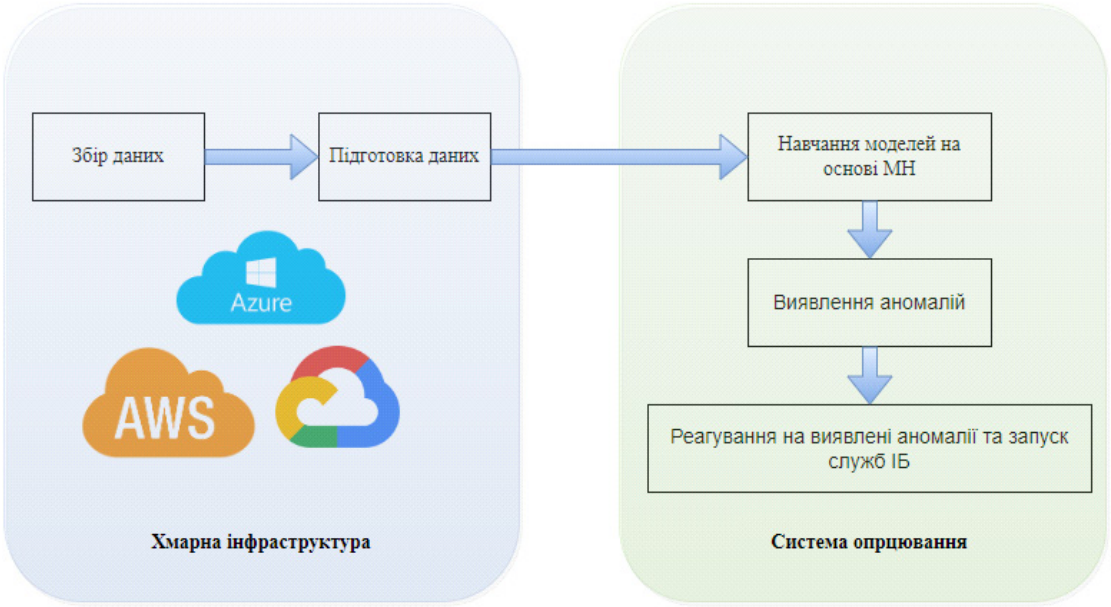

Рис. 1. Схема взаємодії хмарної інфраструктури та інстансів у системі виявлення аномалій ІБ на основі застосування методів МН

На рисунку 1 схематично показано взаємодію хмарної інфраструктури та інстансів у системі виявлення аномалій ІБ на основі застосування методів МН. Така взаємодія може бути реалізована у кілька етапів.

Етап 1. Збір даних.

Хмарна інфраструктура надає середовище для розгортання та виконання інстансів, які можуть бути використані для виконання різних завдань та програм. У процесі роботи інстанси генерують дані про поведінку, такі як використання ресурсів, мережевий трафік, журнали подій тощо.

Етап 2. Підготовка даних.

Дані, зібрані з інстансів, обробляються та готуються до аналізу. Це може включати очистку даних, масштабування ознак, перетворення форматів і т.д.

Етап 3. Навчання моделей з урахуванням МН.

На основі підготовлених даних будуються моделі МН виявлення аномалій. Ці моделі можуть включати алгоритми класифікації, кластеризації, дерева рішень, та ін, здатні виявляти незвичайні або підозрілі патерни в даних.

Етап 4. Виявлення аномалій.

Навчені моделі застосовуються до нових даних, що надходять від інстансів хмарних обчислень, виявлення аномалій. Це може включати аналіз аномальних шаблонів використання ресурсів, незвичайних мережевих пакетів, незапланованих подій у журналах та інших незвичайних сценаріїв.

Етап 5. Реагування на виявлені аномалії.

Після виявлення аномалій система ІБ може вживати різних заходів реагування, таких як надсилання повідомлень адміністраторам, блокування доступу до ресурсів, запуск додаткових заходів безпеки тощо.

У даній структурній схемі, взаємодія між хмарною інфраструктурою, та інстансами в системі виявлення аномалій ІБ, засноване на зборі та аналізі даних від інстансів, з подальшим навчанням моделей МН для виявлення аномалій та вжиття відповідних заходів щодо забезпечення ІБ. Таким чином, інстанси хмарної інфраструктури відіграють ключову роль у забезпеченні ІБ хмарних сервісів, забезпечуючи ізоляцію, моніторинг, керування доступом та захист від мережевих атак. Використання методів МН для виявлення аномалій в інстансах хмарної інфраструктури, може бути ефективним способом виявлення незвичайних або шкідливих дій, які можуть загрожувати безпеці системи. Однак, зазначимо, що для ІБ хмарних сервісів у такій схемі можуть мати місце деякі відмінності. Що пов'язано з такими чинниками:

- Рівень абстракції. Хмарні послуги надають абстрактніший рівень доступу до обчислювальних ресурсів, ніж просто хмарна інфраструктура. Користувачі хмарних сервісів часто мають справу з більш високорівневими сервісами, такими як платформи як сервіс (PaaS), програмне забезпечення як сервіс

(SaaS) і т.д. Це може вплинути на способи збирання та аналізу даних для виявлення аномалій, оскільки доступ до низькорівневих деталей інфраструктури може бути обмежений.

• Типи даних. У хмарних сервісів можуть генеруватися різні типи даних, наприклад, дані про взаємодію користувачів з додатками або обробку транзакцій. Відповідно методи виявлення аномалій можуть бути спрямовані на аналіз цих специфічних типів даних.

• Інтеграція з API. Багато хмарних сервісів надають API для взаємодії з ними. Використання таких API може полегшити збирання даних для виявлення аномалій та інтеграцію із системами ІБ.

• Керування доступом та ІБ. Багато хмарних сервісів мають власні механізми керування доступом і заходи безпеки, які можуть впливати на способи виявлення аномалій. Наприклад, наявність механізмів автентифікації та авторизації може сприяти ідентифікації підозрілих активностей.

Відповідно, взаємодія з хмарними сервісами може вимагати врахування специфічних особливостей цих сервісів та адаптацію методів виявлення аномалій відповідно до їх характеристик.

Як було показано в [15, 17, 21, 28, 36] методи МН, такі як алгоритми кластеризації або методи спостереження без вчителя (наприклад, метод головних компонентів), можуть використовуватися для аналізу поведінки інстансів хмарної інфраструктури та виявлення аномалій. Наприклад, якщо виявляється незвичайна активність у використанні ресурсів або мережному трафіку, це може вказувати на можливу атаку або порушення ІБ.

Відповідно до [15] методи МН можуть використовуватися для аналізу системних параметрів інстансів хмарної інфраструктури, таких як завантаження процесора, використання пам'яті, дискова активність тощо.

У [28] наголошується, що методи навчання з вчителем можуть бути застосовані для аналізу журналів подій (логів) інстансів хмарної інфраструктури з метою виявлення аномальних чи підозрілих дій. Наприклад, можна навчити модель класифікації з урахуванням ретроспективних даних про події визначення, які події є нормальними а які – аномальними.

Методи МН можуть бути застосовані для аналізу мережевого трафіку інстансів хмарної інфраструктури з метою виявлення аномальних патернів або атак. Наприклад, можна використовувати алгоритми виявлення викидів для виявлення незвичайної мережевої поведінки, яка може вказувати на атаку або наявність шкідливого програмного забезпечення [17, 21].

Як показав аналіз попередніх досліджень, у зв'язку з міграцією все більшого обсягу даних та додатків у хмарні сервіси, ІБ стикається з низкою нових та унікальних викликів. Таблиця 1 містить систематизований огляд основних загроз, із якими зіткнулися організації під час використання хмарних сервісів.

Таблиця 1

Систематизація основних загроз, з якими зіткнулися організації під час використання хмарних сервісів (складено автором за результатами аналізу літературних джерел, наведених у цьому дослідженні)

Загроза для ІБ хмарного сервісу	Пріоритетні заходи щодо нівелювання загрози
Недостатній контроль над обліковими записами, правами, доступом та паролями у хмарних сервісах	Дискретна ізоляція користувачів та додатків. Ефективні інструменти управління правами доступу. Багатофакторна автентифікація (MFA). Керування доступом на основі ролей (RBAC). Аудит доступу та моніторинг з метою виявлення підозрілих активностей та НСД чи спроби вторгнення в реальному часі.
Інтерфейси та API з недостатнім захистом	Проведення регулярного аудиту та оцінки безпеки інтерфейсів та API допоможе виявити потенційні вразливості та недоліки в їх реалізації. Використання стандартів безпеки, таких як OAuth, OpenID Connect, SSL/TLS, а також відповідність принципам RESTful API допомагає забезпечити захист при роботі з інтерфейсами та API хмарних сервісів. Реалізація суворої системи авторизації для доступу до API допоможе запобігти НСД до хмарного сервісу та захистить дані від витоків.
Некоректна конфігурація та недостатнє керування змінами у хмарному сервісі.	Використання засобів автоматизації для налаштування та керування конфігурацією хмарними сервісами допоможе запобігти людським помилкам та забезпечити стандартизацію налаштувань ІБ. Проведення регулярних аудитів конфігурації хмарного сервісу допоможе виявляти та виправляти потенційні вразливості та помилки конфігурації. Впровадження систем моніторингу змін дозволить відстежувати та аналізувати всі зміни, що вносяться до хмарного сервісу, що сприятиме оперативному виявленню несанкціонованих дій та запобігатиме загрозам ІБ хмарного сервісу. Розробка та впровадження суворих політик ІБ, включаючи правила конфігурації та процедури керування змінами, допоможе мінімізувати ризики місконфігурації та несанкціонованих змін.

Продовження таблиці 1

Загроза для ІБ хмарного сервісу	Пріоритетні заходи щодо нівелювання загрози
Проблеми безпеки, пов'язані з архітектурою хмарних систем	При розгляді бізнес-цілей, ризиків, загроз ІБ та відповідності законодавству в контексті хмарногих сервісів, а також особливостям їх інфраструктури, об'єктам інформаційної діяльності слід врахувати високу динаміку змін та обмежений централізований контроль у хмарних сховищах. Необхідно акцентувати увагу на розвитку та адаптації інфраструктурної стратегії хмарних сервісів. При адаптації рішень необхідно враховувати основні практики оцінки ІБ, що надаються вендором.
Загрози та ризики, пов'язані з розробкою додатків для хмарних сервісів	Забезпечення навчання та сертифікації розробників з безпечної розробки додатків для хмарних сервісів допоможе підвищити обізнаність з ІБ та знизити ризик помилок у коді. При розробці програм для хмарних сервісів слід використовувати перевірені фреймворки та бібліотеки, які мають вбудовані механізми безпеки та пройшли перевірку на вразливості. Проведення статичного та динамічного аналізу коду допоможе виявляти потенційні вразливості та помилки у додатках ще на стадії розробки. Налаштування програм з урахуванням принципів захисту за промовчанням, таких як мінімізація привілеїв та обмеження доступу до ресурсів, допоможе знизити поверхню атаки та зменшити ризик компрометації системи.
Загрози та вразливості, що виникають під час роботи з хмарними сервісами, що надаються зовнішніми компаніями	Перед використанням хмарних сервісів необхідно провести ретельний аналіз безпеки постачальника, включаючи його репутацію, стандарти безпеки, сертифікації та рейтинги надійності. Важливо укласти SLA (Service Level Agreement), в якому мають бути чітко визначені зобов'язання постачальника в галузі безпеки, включаючи процедури реагування на інциденти, резервне копіювання даних та доступ до аудиту. Здійснення регулярного моніторингу та аудиту ІБ дозволить виявляти потенційні вразливості та недоліки у безпеці хмарних сервісів, а також контролювати їхню відповідність стандартам безпеки. Розробка та регулярне оновлення плану реагування на інциденти дозволить оперативно та ефективно реагувати на можливі загрози ІБ в хмарних сервісах.
Загрози, пов'язані з системними вразливостями у хмарних сервісах	Необхідно регулярно оновлювати та патчити всі компоненти хмарної інфраструктури, включаючи операційні системи, програми та сервіси, щоб виправити відомі вразливості. Проведення регулярного сканування та моніторингу вразливостей у хмарній інфраструктурі допоможе оперативно виявляти та усувати потенційні загрози ІБ. Обмеження доступу та привілеїв до системних ресурсів та даних у хмарних сервісах допоможе знизити ризик експлуатації вразливостей.
Загрози, пов'язані з ненавмисним витіканням інформації з хмарного сховища	Необхідно провести перевірку баз даних (БД) PaaS, сховищ та БД, розміщених на хостингу, включаючи ВМ, контейнери (інстанси) та встановлене на них програмне забезпечення. Слід вибирати пошукові машини, які повністю інтегровані у хмарне середовище, для того, щоб своєчасно виявити будь-які кореневі або мережеві сервіси, що роблять трафік видимим ззовні. Ці заходи також включають балансувальники навантаження, мережі доставки контенту, мережевий піринг (network peering) та хмарні фаєрволи. Пошукова машина повинна враховувати безліч мережевих компонентів, таких як кластерні IP, сервіси Kubernetes та правила доступу.
Загрози, пов'язані з некоректною конфігурацією та застосуванням безсерверних та контейнерних рішень	Використання засобів автоматизації конфігурації та деплойменту, таких як Ansible, Terraform або Kubernetes, допоможе запобігти людським помилкам при налаштуванні та розгортанні контейнерів та безсерверних додатків. Впровадження систем моніторингу та аудиту конфігурації дозволить своєчасно виявляти та виправляти місконфігурації в реальному часі, а також відстежувати зміни у конфігурації для виявлення потенційних уразливостей в ІБ хмарних сервісів. Також ефективним може бути застосування принципів least privilege, оскільки налаштування прав доступу та привілеїв для контейнерів та безсерверних функцій згідно з принципом "найменших привілеїв" допоможе знизити ризик експлуатації вразливостей.

Закінчення таблиці 1

Загроза для ІБ хмарного сервісу	Пріоритетні заходи щодо нівелювання загрози
Загрози, пов'язані з діями організованих злочинних груп та/або хакерських угруповань	Встановлення засобів захисту мережі, firewalls, системи виявлення вторгнень (IDS) та системи запобігання вторгненням (IPS), а також регулярний моніторинг мережного трафіку для виявлення аномальної активності. Впровадження багаторівневої автентифікації та суворого контролю доступу до хмарних ресурсів, включаючи механізми двохфакторної автентифікації, обмеження доступу за ролями та привілеями, а також регулярне оновлення паролів. Застосування шифрування даних у спокої та під час їх передачі між клієнтами та хмарними сервісами допоможе захистити конфіденційну інформацію від НСД. Проведення регулярних аудитів ІБ та моніторингу подій для виявлення та реагування на потенційні загрози та інциденти ІБ у реальному часі. Регулярне створення резервних копій даних та розробка планів відновлення після інцидентів допоможе мінімізувати втрату даних у разі атаки або інциденту ІБ.
Загрози, пов'язані з ексфільтрацією даних хмарних сховищ	Налаштування прав доступу до хмарних сховищ відповідно до принципу "необхідності" (least privilege), коли тільки необхідним користувачам та групам має надаватися доступ до даних. Впровадження систем моніторингу активності та виявлення загроз дозволить виявляти аномальну активність у хмарних сховищах даних, таку як незвичайні спроби доступу або завантаження великих обсягів даних. Впровадження систем запобігання витоку даних (DLP), які можуть автоматично виявляти та блокувати спроби несанкціонованого експорту або завантаження конфіденційної інформації з хмарних сховищ. Проведення навчання та тренінгів для співробітників за правилами безпечного поводження з даними у хмарних сховищах, а також щодо розпізнавання та запобігання соціальній інженерії та фішингових атак.

Майбутні напрями досліджень.

У роботах, які були проаналізовані у даній статті, переважно обговорюється коло питань, присвячених проблемі комплексного підходу до забезпечення ІБ хмарних інфраструктур. Як показано в більшості робіт, хмарні обчислення стрімко набирають популярності, витісняючи традиційні моделі ведення бізнес-процесів для об'єктів інформатизації. Проте, проаналізовані роботи недостатньо охоплюють питання реалізації системи моніторингу розподілу ресурсів. Також було виявлено, що значною мірою розглянуті роботи не торкаються такого аспекту забезпечення інформаційної безпеки хмарних інфраструктур, як застосування методів МН та для створення прогнозної моделі завантаження та методики збору метрик ІБ інстансів. Серед основних питань, які потребують вирішення у рамках майбутніх досліджень, слід виділити:

– розробку нових моделей, що описують аномальну поведінку інстансів, внаслідок порушення політики ІБ;

– розвиток методів МН з вчителем для аналізу журналів подій (логів) інстансів хмарної інфраструктури з метою виявлення аномальних чи підозрілих дій.

Висновки.

Показано, що хмарні обчислення забезпечують доступ до мережевих ресурсів, таких як сховища даних та обчислювальні потужності, на запит, без прямого управління з боку користувачів. В даний час хмарні обчислення включають як публічні, так і приватні центри обробки даних (ЦОД), що надають клієнтам єдину платформу через інтернет. Мобільні хмарні обчислення використовують розподілені обчислення для передачі програм на мобільні пристрої, такі як телефони та планшети.

Встановлено, що численні дослідження вказують на проблеми інформаційної безпеки (ІБ), загрози та вразливості для клієнтів, з якими стикаються хмарні обчислення та мобільні хмарні обчислення, та одним із перспективних методів боротьби з цими загрозами є використання методів машинного навчання (далі МН).

Проведено аналіз загроз та проблем з ІБ хмарних структур, а також огляд рішень, запропонованих різними авторами, щодо забезпечення безпеки хмарних обчислень та хмарних сервісів. Насамперед, розглянуто дослідження, що ґрунтуються на застосуванні алгоритмів МН для забезпечення безпеки хмарних обчислень та хмарних сервісів.

Список використаних джерел:

1. Горбань О., Браіловський М. Захист хмарної інфраструктури від DDoS атак. Проблеми кібербезпеки інформаційно-телекомунікаційних систем: Збірник матеріалів доповідей та тез; м. Київ, 27-28 жовтня 2022 року; Київський національний університет імені Тараса Шевченка / Редкол.: В.В. Ільченко. (голова) та ін. – К.: ВПЦ «Київський університет», 2022. 159 с.

2. Маковоз К. О. Методи виявлення вторгнень у хмарних системах відеоспостереження. Хмарні технології в освіті: матеріали Всеукраїнського науково-методичного Інтернет-семінару (Кривий Ріг–Київ–Черкаси–Харків, 21 грудня 2012 р.). – Кривий Ріг: Видавничий відділ КМІ, 2012. 173 с.

3. Фролов В. В. Analysis of approaches providing security of cloud sevices. Radioelectronic and Computer Systems, 2020. (1), 70-82.
4. Шимчук Г., Голотенко О., Золотий Р. З. Основні проблеми та загрози хмарної безпеки. Матеріали науково-технічної конференції «Інформаційні моделі, системи та технології» Тернопільського національного технічного університету імені Івана Пулюя, 2022. 59–60.
5. Aawadallah N. Security Threats of Cloud Computing. Int. J. Recent Innov. Trends Comput. Commun. 2015, 3, 2393–2397.
6. Al-Janabi S., Shehab A. Edge Computing: Review and Future Directions. REVISTA AUS J. 2019, 26, 368–380.
7. Alsolami E. Security threats and legal issues related to Cloud based solutions. Int. J. Comput. Sci. Netw. Secur. 2018, 18, 156–163.
8. Barona R., Anita M. A survey on data breach challenges in cloud computing security: Issues and threats. In Proceedings of the International Conference on Circuit, Power and Computing Technologies (ICCPCT), Paris, France, 17–18 September 2017; pp. 1–8.
9. Bhamare D., Salman T., Samaka M., Erbad A., Jain, R. Feasibility of Supervised Machine Learning for Cloud Security. In Proceedings of the International Conference on Information Science and Security, Jaipur, India, 16–20 December 2016; pp. 1–5.
10. Borylo P., Tornatore M., Jaglarz P., Shahriar N., Cholda P., Boutaba R. Latency and energy-aware provisioning of network slices in cloud networks. Comput. Commun. 2020, 157, 1–19.
11. Butt U. A., Mehmood M., Shah S. B. H., Amin R., Shaukat,M. W., Raza S. M., Piran M. J. A review of machine learning algorithms for cloud computing security. Electronics, 2020. 9(9), 1379.
12. Callara M., Wira P. User Behavior Analysis with Machine Learning Techniques in Cloud Computing Architectures. In Proceedings of the 2018 International Conference on Applied Smart Systems, Médéa, Algeria, 24–25 November 2018; pp. 1–6.
13. Carmo M., Dantas Silva F. S., Neto A.V., Corujo D., Aguiar, R. Network-Cloud Slicing Definitions for Wi-Fi Sharing Systems to Enhance 5G Ultra-Dense Network Capabilities. Wirel. Commun. Mob. Comput. 2019, 2019, 8015274.
14. Deshpande P., Sharma S. C., Peddoju S. K. Security threats in cloud computing. In Proceedings of the International Conference on Computing, Communication and Automation, Greater Noida, India, 11–14 December 2011; pp. 632–636.
15. Elzamly A., Hussin B., Basari, A. S. Classification of Critical Cloud Computing Security Issues for Banking Organizations: A Cloud Delphi Study. Int. J. Grid Distrib. Comput. 2016, 9, 137–158.
16. Kazim M., Zhu S. Y. A survey on top security threats in cloud computing. Int. J. Adv. Comput. Sci. Appl. 2015, 6.
17. Khan A. N., Fan M. Y., Malik A., Memon R. A. Learning from Privacy Preserved Encrypted Data on Cloud Through Supervised and Unsupervised Machine Learning. In Proceedings of the International Conference on Computing, Mathematics and Engineering Technologies, Sindh, Pakistan, 29–30 January 2019; pp. 1–5.
18. Khan M. A survey of security issues for cloud computing. J. Netw. Comput. Appl. 2016, 71, 11–29.
19. Khilar P., Vijay C., Rakesh S. Trust-Based Access Control in Cloud Computing Using Machine Learning. In Cloud Computing for Geospatial Big Data Analytics; Das, H., Barik, R., Dubey, H., Roy, D., Eds.; Springer: Cham, Switzerland, 2019; Volume 49, pp. 55–79.
20. Le Duc T., Leiva R. G., Casari P., Östberg, P. O. Machine Learning Methods for Reliable Resource Provisioning in Edge-Cloud Computing: A Survey. ACM Comput. Surv. 2019, 52, 1–39.
21. Lee Y., Yongjoon P., Kim, D. Security Threats Analysis and Considerations for Internet of Things. In Proceedings of the International Conference on Security Technology (SecTech), Jeju Island, Korea, 25–28 November 2015; pp. 28–30.
22. Lim S. Y., Kiah M. M., Ang T. F. Security Issues and Future Challenges of Cloud Service Authentication. Polytech. Hung. 2017, 14, 69–89.
23. Lin C., Lu H. Response to Co-resident Threats in Cloud Computing Using Machine Learning. In Proceedings of the International Conference on Advanced Information Networking and Applications, Caserta, Italy, 15–17 April 2020; Volume 926, pp. 904–913.
24. Mathkunti N. Cloud Computing: Security Issues. Int. J. Comput. Commun. Eng. 2014, 3, 259–263.
25. Nadeem M. Cloud Computing: Security Issues and Challenges. J. Wirel. Commun. 2016, 1, 10–15.
26. Salah K., Hammoud M., Zeadally, S. Teaching cybersecurity using the cloud. IEEE Transactions on Learning Technologies, 2015. 8(4), 383–392.
27. Sarma M., Srinivas Y., Ramesh N., Abhiram, M. Improving the Performance of Secure Cloud Infrastructure with Machine Learning Techniques. In Proceedings of the International Conference on Cloud Computing in Emerging Markets (CCEM), Bangalore, India, 19–21 October 2016; pp. 78–83.
28. Sayantan G., Stephen Y., Arun-Balaji B. Attack Detection in Cloud Infrastructures Using Artificial Neural Network with Genetic Feature Selection. In Proceedings of the IEEE 14th International Conference on Dependable, Autonomic and Secure Computing, Athens, Greece, 12–15 August 2016; pp. 414–419.
29. Selamat N., Ali F. Comparison of malware detection techniques using machine learning algorithm. Indones. J. Electr. Eng. Comput. Sci. 2019, 16, 435.
30. Stefan H., Liakat M. Cloud Computing Security Threats And Solutions. J. Cloud Comput. 2015, 4, 1.
31. Subashini S., Kavitha V. A Survey on Security Issues in Service Delivery Models of Cloud Computing. J. Netw. Comput. Appl. 2011, 35, 1–11.
32. Sulistio A., Reich C., Doelitzscher, F. Cloud infrastructure & applications–CloudIA. In Cloud Computing: First International Conference, CloudCom 2009, Beijing, China, December 1-4, 2009. Proceedings 1 (pp. 583–588). Springer Berlin Heidelberg.
33. Varun K. A., Rajkumar N., Kumar N. K. Survey on security threats in cloud computing. Int. J. Appl. Eng. Res. 2014, 9, 10495–10500.
34. Venkatraman S., Mamoun A. Use of data visualisation for zero-day malware detection. Secur. Commun. Netw. 2018, 1–13.
35. Xue M., Yuan C., Wu H., Zhang Y., Liu W. Machine Learning Security: Threats, Countermeasures, and Evaluations. IEEE Access 2020, 8, 74720–74742.
36. Yau S. S., Buduru A. B., Nagaraja, V. Protecting critical cloud infrastructures with predictive capability. In 2015 IEEE 8th International Conference on Cloud Computing (2015, June). (pp. 1119-1124). IEEE.
37. Yuhong L., Yan S., Jungwoo R., Syed R., Athanasios V. A Survey of Security and Privacy Challenges in Cloud Computing: Solutions and Future Directions. J. Comput. Sci. Eng. 2015, 9, 119–133.